

Robocall Mitigation Program Description

Introduction

OPERADORA DE PROYECTOS NEURONA S. de R.L. de C.V. (the **Company**), based in Mexico, is a voice service provider offering telecommunications services primarily for access control systems and their users. This document provides a comprehensive description of the Company's Robocall Mitigation Program, as required for its filing in the FCC's Robocall Mitigation Database. It outlines the specific measures the Company has in place to prevent and mitigate the origination of illegal robocalls on its network. The Company's robocall mitigation practices have been fully implemented since **January 2025**, and the Company remains committed to complying with all FCC regulations in this regard.

Company Services and Caller ID Controls

Service Overview: The Company's voice service is utilized by end users, resellers, and enterprise clients for critical communication between access control devices and the intended recipients. For example, when a visitor uses an access control or intercom device at a secured facility (such as a residential gate or office entrance), the system places a call through the Company's network to reach the authorized user's phone. These calls are generally person-to-person communications initiated by a physical device or system event, not by mass dialing or automated telemarketing systems. This specialized use case inherently limits call volumes and the potential for abuse, as calls occur only in response to specific user actions (e.g. someone requesting access at a gate).

Caller ID Authorization: The Company strictly controls the Caller ID information that can be used on outbound calls. Clients (including end users, resellers, or companies using our platform) **cannot arbitrarily set or spoof Caller ID values**. Instead, the Company employs a **numeric code authentication system** to verify any telephone number a client wishes to use as Caller ID. Before a new Caller ID is authorized on our network, the client must prove they have control of that number: the client is required to initiate a special configuration call from the phone number in question and enter a one-time verification code provided by the Company. Only upon successful entry of the correct code (thereby confirming the caller's access to that number) will the system permit that number to be used as the Caller ID for future calls. This procedure ensures that **telephone numbers are authenticated and linked to the legitimate user**. It prevents users (or their downstream customers, in the case of resellers) from impersonating or misusing numbers that are not rightfully theirs. By enforcing this Caller ID verification step, the Company mitigates the risk of Caller ID spoofing, a common tactic in illegal robocalling.

Controlled Caller ID and Assignment: In many cases, the Caller ID numbers used for calls are ones **assigned by the Company** to the client’s device or account, or they are numbers that the client has verified and registered through the above process. Clients cannot use unverified external numbers. All outbound calls, therefore, carry identifying information that has been vetted. This control greatly reduces the likelihood that malicious actors could inject random or misleading caller identities into calls routed by our service. It also provides traceability, since each authorized Caller ID is tied to a specific client or device in our records.

Robocall Mitigation Practices

The Company has implemented several layers of precautions and procedures as part of its Robocall Mitigation Program. These measures are designed to **avoid originating illegal robocall traffic** to the maximum extent reasonable given the Company’s size and the nature of its services. Key components of our mitigation program include:

- **Limited Service Scope & Low Call Volume:** The nature of the Company’s service inherently limits the volume and rate of calls. Communications are generally one-to-one (device to user) and occur only when triggered by an access event. There is no capability for a customer to run high-volume telemarketing or auto-dialing campaigns through our systems. Furthermore, each client or device is intrinsically limited in concurrent calling capacity (often one call at a time per device or user account). This **limited use case** greatly diminishes the risk of mass robocall traffic originating from our network.
- **Customer Vetting and Accountability:** All clients of the Company are known parties—either direct end users, authorized resellers, or business customers under contract. New customers must provide identifying information and agree to the Company’s terms of service and acceptable use policies, which **prohibit the initiation of illegal or spam calls**. For business clients and resellers, the Company collects relevant details such as business name, contact persons, and intended use of the service. By having a direct relationship with each client (or through a vetted reseller), the Company maintains accountability for who is using its network. Foreign-originated traffic from unknown third parties is not accepted; only our registered clients and their verified devices may originate calls, and all must adhere to applicable laws. This **“know-your-customer”** approach helps ensure that the traffic on our network comes from legitimate, accountable users rather than anonymous sources.
- **Caller ID Verification Controls:** As described in the previous section, the Company requires verification of any Caller ID before use. This **white-listing** of caller numbers (post-verification) means customers can only use numbers that have been validated as theirs or assigned by the Company. By ensuring callers use only authorized numbers, we prevent one of the common avenues for illegal robocallers – namely, injecting random or misleading caller IDs to trick call recipients – from occurring on our platform. Every outbound call on our network carries a Caller ID that has been vetted and linked to a customer account, providing **transparency and traceability**.

- **Call Detail Record Retention:** The Company's phone system (PBX) automatically logs detailed information for every outbound call. These **Call Detail Records (CDRs)** include data such as the originating trunk or device, the dialed destination number, the Caller ID presented, call timestamp, and call duration. CDRs are securely stored and maintained for a significant period of time in accordance with industry practices. Maintaining these records allows the Company to review and analyze calling patterns when needed. In the ordinary course of business, we do not inspect every call record in real time; however, the data is readily available should any questions arise regarding particular calls or calling trends. This log retention is crucial for both internal review and external compliance (e.g., responding to FCC or law enforcement inquiries).
- **No Real-Time Robocall Analytics (Current Limitations):** At present, the Company **does not utilize an automated system for real-time detection or blocking of suspected robocalls**, and it does not have a dedicated abuse monitoring team. Given our relatively small scale and the low-risk profile of our service, we have determined that real-time analytics tools (which are often used by larger carriers to scan for spam call patterns) are not currently necessary. Instead, the Company's strategy relies on preventative measures (like caller ID authentication and customer vetting) and reactive measures in response to any specific incidents. The **technical staff** do monitor the network's overall performance and will notice if there are any unusual surges or anomalies in call traffic volumes. If any **complaint or indication of illegal calling** involving our network is received (for example, if a call is reported as a suspected unlawful robocall or we receive an abuse report), the Company will promptly investigate using its stored call records. In summary, while we lack automated spam-detection systems, we compensate by tightly controlling access to our system and being ready to investigate and address issues if they arise.
- **Enforcement and Remedial Action:** In the event that a customer of the Company is found to be **originating illegal robocalls or violating our service terms**, we will take swift and decisive action to mitigate any further harm. Such actions may include suspending the customer's access to our voice service, terminating the customer's account or contract, and/or blocking the specific offending call traffic. The Company's service agreements and policies give us the right to suspend or terminate service for any customer engaging in prohibited activities (which include illegal robocalling or fraudulent calling schemes). By enforcing these consequences, we ensure that any source of abusive calls is quickly cut off from our network. Additionally, the Company will report egregious violations to the appropriate authorities as required. This commitment to enforcement acts as a deterrent against any misuse of our system and demonstrates that we will not tolerate our platform being used for unlawful purposes.

Traceback Compliance and Cooperation

The Company fully **cooperates with FCC officials and the Industry Traceback Group (ITG)** in efforts to identify and stop illegal robocalls. We acknowledge that, under FCC rules, we are obligated to respond to official traceback requests and we take this obligation very seriously. Our procedures for traceback compliance are as follows:

- **Designated Contact:** The Company has designated an official point of contact for all robocall mitigation and traceback inquiries, as provided in our Robocall Mitigation Database filing. This contact information (including phone number and email) is kept up-to-date and is monitored by the Company's compliance personnel. Any traceback request or communication from the FCC or authorized traceback consortium will reach our designated contact, ensuring that such requests receive immediate attention.
- **Prompt Response to Traceback Requests:** Upon receiving a traceback request (a request to investigate and report the source of a suspicious or illegal call that has been traced into our network), the Company **promptly investigates and responds** with the required information. In practice, we strive to provide all requested data as quickly as possible – typically responding well within one business day of receipt of the request, often much sooner. The Company understands the urgency of these requests in combating illegal calls, and thus we prioritize them in our workflow.
- **Information Provided:** In response to a traceback inquiry, the Company will retrieve **all relevant outbound call information** from our PBX and CDR logs pertaining to the specific call(s) in question. This generally includes details such as the date and time of the call, the calling and called numbers, the Caller ID that was presented, the identifier of the trunk or device that originated the call on our system, and any other pertinent routing information we have. We will also identify the customer or client on whose behalf the call was placed (e.g., which end-user or reseller's account originated the traffic). This information is compiled and returned to the requesting authority in the format they require, ensuring that the traceback can continue down the chain to ultimately find the source of the call.
- **Verification Process:** When preparing the traceback response, the Company takes care to verify the accuracy of the data provided. We cross-check the records in our system to ensure we are isolating the correct call (or range of calls) referenced by the traceback request. If any clarifications are needed (for example, if the identifying data from the requester doesn't immediately match our records), our team will engage to resolve those discrepancies quickly. Our goal is to furnish a **complete and accurate report** to the traceback coordinators so that no time is lost in the enforcement effort.
- **Ongoing Cooperation:** Beyond individual traceback requests, the Company is committed to ongoing cooperation with regulators and law enforcement. We participate in the broader industry initiatives to curb illegal robocalls to the extent our resources allow. If the FCC or other enforcement bodies seek additional information or follow-up on a particular case involving our network, we continue to assist fully. In addition, if patterns or perpetrators of illegal calling are identified, the Company will take internal steps (as described in the enforcement section above) to ensure those actors cannot continue to use our platform. We view ourselves as a proactive partner in the fight against illegal robocalling, despite our small size and niche service area, and we remain vigilant in this role.

Ongoing Commitment and Program Maintenance

The Company affirms that it will **continuously maintain and improve** this Robocall Mitigation Program as needed. We periodically review the effectiveness of our policies and the changing nature of robocall threats. If new technologies or methods become available that would enhance our ability to block or filter illegal calls (such as improved analytics or participation in industry traceback initiatives), we will consider incorporating them into our program in a manner appropriate for our scale of operations. We are also prepared to update our Robocall Mitigation Database filing or this program description if our practices change or if required by updated FCC rules. In all cases, the Company's mission is to provide reliable communication services for legitimate use while doing its part to protect consumers and the public from the scourge of illegal robocalls. We remain committed to compliance, cooperation, and continual improvement in robocall mitigation.

Certification (Declaration under Penalty of Perjury)

OPERADORA DE PROYECTOS NEURONA S. de R.L. de C.V. hereby affirms that all statements made in this Robocall Mitigation Program Description are true, correct, and complete to the best of our knowledge. The Company acknowledges that this certification is made **under penalty of perjury**, and the undersigned representative is legally authorized to make this declaration on the Company's behalf. This affirmation is executed on the date indicated below, with the understanding that false statements or misrepresentations to the Federal Communications Commission are subject to enforcement action under federal law.

Executed on: May 21, 2025 Authorized Representative, OPERADORA DE PROYECTOS NEURONA S. de R.L. de C.V.